HDE03320J EP

PCT/IB04/50850

Europäisches Patentamt | European Patent Office | Office européen des brevets

REC'D 22 JUN 2004
WIPO PCT

Bescheinigung Certificate Attestation

Die angehefteten Unterlagen stimmen mit der ursprünglich eingereichten Fassung der auf dem nächsten Blatt bezeichneten europäischen Patentanmeldung überein.

The attached documents are exact copies of the European patent application described on the following page, as originally filed.

Les documents fixés à cette attestation sont conformes à la version initialement déposée de la demande de brevet européen spécifiée à la page suivante.

Patentanmeldung Nr. Patent application No. Demande de brevet n°

03101719.7

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

Der Präsident des Europäischen Patentamts;
Im Auftrag

For the President of the European Patent Office

Le Président de l'Office européen des brevets
p.o.

R C van Dijk

Anmeldung Nr:
Application no.: 03101719.7
Demande no:

Anmeldetag:
Date of filing: 12.06.03
Date de dépôt:

Anmelder/Applicant(s)/Demandeur(s):

Philips Intellectual Property & Standards
GmbH
Steindamm 94
20099 Hamburg
ALLEMAGNE
Koninklijke Philips Electronics N.V.
Groenewoudseweg 1
5621 BA Eindhoven
PAYS-BAS

Bezeichnung der Erfindung/Title of the invention/Titre de l'invention:
(Falls die Bezeichnung der Erfindung nicht angegeben ist, siehe Beschreibung.
If no title is shown please refer to the description.
Si aucun titre n'est indiqué se referer à la description.)

AES-Coprozessor und Verfahren zur AES-Berechnung

In Anspruch genommene Priorität(en) / Priority(ies) claimed /Priorité(s) revendiquée(s)
Staat/Tag/Aktenzeichen/State/Date/File no./Pays/Date/Numéro de dépôt:

Internationale Patentklassifikation/International Patent Classification/
Classification internationale des brevets:

H04L9/00

Am Anmeldetag benannte Vertragstaaten/Contracting states designated at date of filing/Etats contractants désignées lors du dépôt:

AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LU MC NL
PT SE SI SK TR RO LI

BESCHREIBUNG

AES-Coprozessor und Verfahren zur AES-Berechnung

Die Erfindung betrifft einen AES-Coprozessor und ein Verfahren zur AES-Berechnung mit den in den Oberbegriffen der Ansprüche 1 und 10 genannten Merkmalen.

Der Rijndael-Algorithmus, welcher von der amerikanischen Normungsbehörde National Institute of Standards and Technology (NIST) als Advanced Encryption Standard (AES) ausgewählt wurde, besteht aus zwei Hauptblöcken: Dem Key-Scheduling-Block zur Berechnung der Schlüssel für die einzelnen Verschlüsselungsrunden und dem eigentlichen Ver- und Entschlüsselungsblock. AES-Coprozessoren existieren bisher in zwei Ausführungen. Es werden entweder sämtliche Rundenschlüssel vor der Ver-/Entschlüsselung berechnet (Pre-Calculation), wobei große Speicherbereiche zur Speicherung der Rundenschlüssel benötigt werden oder die Rundenschlüssel werden vor der jeweiligen Verschlüsselungsrunde berechnet, wodurch bekannt ist, zu welchem Zeitpunkt ein Rundenschlüssel berechnet wird und somit eine Attacke auf die Schlüsselerzeugung leichter ist. Da bei der Schlüsselerzeugung ein rekursiver Algorithmus verwendet wird, wird auch hier ein größerer Speicherbereich benötigt.

Aufgabe der Erfindung ist es, einen AES-Coprozessor und ein Verfahren zur AES-Berechnung zu schaffen, welche sich durch einen geringeren Speicherbedarf und eine höhere Sicherheit gegen Attacken auf die Rundenschlüsselerzeugung als bisher bekannt auszeichnen.

Diese Aufgabe wird erfindungsgemäß durch einen AES-Coprozessor mit den in Anspruch 1 genannten Merkmalen und ein Verfahren zur AES-Berechnung mit den in Anspruch 10 genannten Merkmalen gelöst. Der erfindungsgemäße AES-Coprozessor ist dadurch charakterisiert, dass eine Steuereinrichtung mit wenigstens einem Ver-/Entschlüsselungsmittel über wenigstens ein Kommunikationsmittel verbunden ist, die Steuereinrichtung mit wenigstens einem Rundenschlüsselerzeugungsmittel über wenigstens ein weiteres Kommunikationsmittel verbunden ist, die Steuereinrichtung

wenigstens einen externen Schlüsseleingang aufweist, das wenigstens eine Ver-/Entschlüsselungsmittel wenigstens einen externen Dateneingang und wenigstens einen externen Datenausgang aufweist und das wenigstens eine Ver-/Entschlüsselungsmittel und das wenigstens eine Rundenschlüsselerzeugungsmittel voneinander entkoppelt sind. Es existieren somit weder ein direkter Datenpfad zwischen dem wenigstens einen Ver-/Entschlüsselungsmittel und dem wenigstens einen Rundenschlüsselerzeugungsmittel, noch eine direkte Verbindung des wenigstens einen Rundenschlüsselerzeugungsmittels zur Außenwelt. Somit kann ein Zugriff auf das wenigstens eine Rundenschlüsselerzeugungsmittel lediglich durch die Ablaufsteuerung oder das wenigstens eine Ver-/Entschlüsselungsmittel erfolgen. Auf diese Weise wird eine erhöhte Sicherheit gegen Attacken auf die Rundenschlüsselerzeugung kombiniert mit einem geringen erforderlichen Speicherbereich, welcher lediglich zur Aufnahme temporär für die rekursive Schlüsselberechnung benötigter Daten dient, erzielt.

In einer bevorzugten Ausgestaltung der Erfindung ist vorgesehen, dass das wenigstens eine Kommunikationsmittel wenigstens eine Anforderungsleitung, wenigstens eine Freigabeleitung und wenigstens eine Datenleitung und/oder das wenigstens eine weitere Kommunikationsmittel wenigstens eine weitere Anforderungsleitung, wenigstens eine weitere Freigabeleitung und wenigstens eine weitere Datenleitung umfasst. Hierdurch werden vorteilhaft besonders günstige Eigenschaften erzielt, wodurch sich der erfindungsgemäße AES-Coprozessor für die einfach handhabbare Implementierung vielfältiger Steueralgorithmen eignet.

Weiterhin ist in einer bevorzugten Ausgestaltung der Erfindung vorgesehen, dass die wenigstens eine Anforderungsleitung, die wenigstens eine Freigabeleitung und die wenigstens eine Datenleitung und/oder die wenigstens eine weitere Anforderungsleitung, die wenigstens eine weitere Freigabeleitung und die wenigstens eine weitere Datenleitung zumindest teilweise dieselbe Leitungsphysik belegen. Auf diese Weise wird vorteilhaft eine Minimierung des erforderlichen Bauraumes und somit eine erhöhte Wirtschaftlichkeit erzielt.

Darüber hinaus ist in einer bevorzugten Ausgestaltung der Erfindung vorgesehen, dass die Steuereinrichtung wenigstens ein Speichermittel umfasst, in welchem wenigstens ein mittels des wenigstens einen Rundenschlüsselerzeugungsmittels erzeugter Rundenschlüssel temporär speicherbar ist. Der erforderliche Speicherbereich ist somit gering und lediglich abhängig von der Rekursionstiefe. Auf diese Weise wird der erforderliche Bauraum minimiert, was in einer erhöhten Wirtschaftlichkeit resultiert.

Ferner ist in einer bevorzugten Ausgestaltung der Erfindung vorgesehen, dass für den Zugriff auf das wenigstens eine Speichermittel wenigstens ein rotierender Zeiger vorgesehen ist. Bereits gelesene Speicherbereiche können so in einfacher Weise zum Beschreiben mit neuen Rundenschlüsseln freigegeben werden, da mit Hilfe der Zeiger keine Bereiche beschrieben werden, die noch nicht gelesen wurden, beziehungsweise ausschließlich Bereiche gelesen werden, die mit gültigen Schlüsselworten beschrieben wurden. Hierdurch kann der benötigte Speicherbereich gering gehalten werden.

Überdies ist in einer bevorzugten Ausgestaltung der Erfindung vorgesehen, dass zur Kommunikation der Steuereinrichtung mit dem wenigstens einen Ver-/Entschlüsselungsmittel und/oder mit dem wenigstens einen Rundenschlüsselerzeugungsmittel wenigstens ein Handshake-Protokoll vorgesehen ist. Hierdurch wird eine temporäre Inaktivität von Ver-/Entschlüsselungsmittel beziehungsweise Rundenschlüsselerzeugungsmittel erzielt, wodurch Attacken auf die Schlüsselerzeugung erschwert werden.

Fernerhin ist in einer bevorzugten Ausgestaltung der Erfindung vorgesehen, dass die Arbeitsweise der Steuereinrichtung, des wenigstens einen Ver-/Entschlüsselungsmittels und des wenigstens einen Rundenschlüsselerzeugungsmittels asynchron zueinander ist. Hierdurch werden Attacken auf die Schlüsselerzeugung erschwert.

In einer bevorzugten Ausgestaltung der Erfindung ist darüber hinaus vorgesehen, dass mittels des wenigstens einen Rundenschlüsselerzeugungsmittels während wenigstens einer inaktiven Phase wenigstens eine Dummy-Berechnung und/oder wenigstens ein Teil wenigstens einer früheren Rundenschlüsselberechnung durchführbar ist. Hierdurch ist ein zusätzlicher Schutz gegen Attacken auf die Schlüsselerzeugung gegeben.

Schließlich ist in einer bevorzugten Ausgestaltung der Erfindung vorgesehen, dass die Zeitspanne zwischen Berechnung und Verwendung des wenigstens einen Rundenschlüssels variabel ist. Hierdurch werden vorteilhaft Attacken auf die Berechnung der Rundenschlüssel erschwert.

Das erfindungsgemäße Verfahren zur AES-Berechnung unter Verwendung eines erfindungsgemäßen AES-Coprozessors zeichnet sich dadurch aus, dass

a) wenigstens ein initialer Schlüssel in eine Steuereinrichtung eingelesen wird,

b) externe Daten in wenigstens ein Ver-/Entschlüsselungsmittel eingelesen werden,

c) wenigstens ein zur Berechnung wenigstens eines Rundenschlüssels benötigtes Datenwort aus wenigstens einem Speichermittel der Steuereinrichtung ausgelesen und zu wenigstens einem Rundenschlüsselerzeugungsmittel transferiert wird,

d) wenigstens ein Rundenschlüssel auf Basis des wenigstens einen Datenwortes mittels des wenigstens einen Rundenschlüsselerzeugungsmittels rekursiv berechnet, zur Steuereinrichtung transferiert und in dem wenigstens einen Speichermittel gespeichert wird,

e) der wenigstens eine Rundenschlüssel zu dem wenigstens einen Ver-/Entschlüsselungsmittel transferiert wird,

f) die externen Daten mittels des wenigstens einen Ver-/Entschlüsselungsmittels unter Verwendung des wenigstens einen Rundenschlüssels verschlüsselt oder entschlüsselt und die ver- beziehungsweise entschlüsselten Daten an wenigstens einem externen Datenausgang bereitgestellt werden und

g) die Schritte b) bis f) so oft wie zur Ver- beziehungsweise Entschlüsselung eines Satzes externer Daten erforderlich wiederholt werden.

Es ist somit weder ein direkter Datenpfad zwischen dem wenigstens einen Ver-/Entschlüsselungsmittel und dem wenigstens einen Rundenschlüsselerzeugungsmittel, noch eine direkte Verbindung des wenigstens einen Rundenschlüsselerzeugungsmittels zur Außenwelt erforderlich. Somit erfolgt ein Zugriff auf das wenigstens eine Rundenschlüsselerzeugungsmittel lediglich durch die Ablaufsteuerung oder das wenigstens eine Ver-/Entschlüsselungsmittel. Auf diese Weise wird eine erhöhte Sicherheit gegen Attacken auf die Rundenschlüsselerzeugung kombiniert mit einem geringen erforderlichen Speicherbereich, welcher lediglich zur Aufnahme temporär für die rekursive Schlüsselberechnung benötigter Daten dient, erzielt.

Im Rahmen des erfindungsgemäßen Verfahrens ist bevorzugt vorgesehen, dass die Kommunikation der Steuereinrichtung mit dem wenigstens einen Ver-/Entschlüsselungsmittel und/oder dem wenigstens einen Rundenschlüsselerzeugungsmittel mittels wenigstens eines Handshake-Protokolls erfolgt. Hierdurch wird eine temporäre Inaktivität von Ver-/Entschlüsselungsmittel beziehungsweise Rundenschlüsselerzeugungsmittel erzielt, wodurch Attacken auf die Schlüsselerzeugung erschwert werden.

Weiterhin ist im Rahmen des erfindungsgemäßen Verfahrens bevorzugt vorgesehen, dass die Kommunikation der Steuereinrichtung mit dem wenigstens einen Ver-/Entschlüsselungsmittel und dem wenigstens einen Rundenschlüsselerzeugungsmittel asynchron erfolgt. Hierdurch werden Attacken auf die Schlüsselerzeugung erschwert.

Darüber hinaus ist im Rahmen des erfindungsgemäßen Verfahrens bevorzugt vorgesehen, dass der Zugriff auf das wenigstens eine Speichermittel mittels wenigstens eines rotierenden Zeigers erfolgt. Bereits gelesene Speicherbereiche können so in einfacher Weise zum Beschreiben mit neuen Rundenschlüsseln freigegeben werden, da mit Hilfe der Zeiger keine Bereiche beschrieben werden, die noch nicht gelesen wurden, beziehungsweise ausschließlich Bereiche gelesen werden, die mit gültigen Schlüsselworten beschrieben wurden. Hierdurch kann der benötigte Speicherbereich gering gehalten werden.

Ferner ist im Rahmen des erfindungsgemäßen Verfahrens bevorzugt vorgesehen, dass mittels des wenigstens einen Rundenschlüsselerzeugungsmittels während wenigstens einer inaktiven Phase wenigstens eine Dummy-Berechnung und/oder wenigstens ein Teil wenigstens einer früheren Rundenschlüsselberechnung durchgeführt wird. Hierdurch ist ein zusätzlicher Schutz gegen Attacken auf die Schlüsselerzeugung gegeben.

Schließlich ist im Rahmen des erfindungsgemäßen Verfahrens bevorzugt vorgesehen, dass die Zeitspanne zwischen Berechnung und Verwendung des wenigstens einen Rundenschlüssels variabel ist. Hierdurch werden vorteilhaft Attacken auf die Berechnung der Rundenschlüssel erschwert.

Weitere bevorzugte Ausgestaltungen der Erfindung ergeben sich aus den übrigen, in den Unteransprüchen genannten Merkmalen.

Die Erfindung wird nachfolgend in Ausführungsbeispielen anhand der zugehörigen Zeichnung, welche einen AES-Coprozessor zeigt, näher erläutert.

In der Figur ist das Blockschaltbild einer Ausführung eines erfindungsgemäßen AES-Coprozessors 10 dargestellt. Der AES-Coprozessor 10 umfasst eine Steuereinrichtung 12, ein Ver-/Entschlüsselungsmittel 14 und ein Rundenschlüsselerzeugungsmittel 18, wobei die Steuereinrichtung 12 mit dem Ver-/Entschlüsselungsmittel 14 über ein Kommunikationsmittel 16 und mit dem Rundenschlüsselerzeugungsmittel 18 über ein weiteres Kommunikationsmittel 20 verbunden ist. Das Kommunikationsmittel 16 und das weitere Kommunikationsmittel 20 weisen jeweils eine Anforderungsleitung und eine Freigabeleitung auf sowie jeweils eine Datenleitung zur Übertragung der Rundenschlüssel, wobei das Rundenschlüsselerzeugungsmittel 18 über eine zusätzliche Datenleitung zur Übertragung von Zwischenergebnissen für die rekursive Berechnung der Rundenschlüssel mit der Steuereinrichtung 12 verbunden ist. Die Steuereinrichtung 12 umfasst ein Speichermittel 28 zur temporären Aufnahme eines über einen externen Schlüsseleingang 22 in die Steuereinrichtung eingebrachten initialen Schlüssels, von

Rundenschlüsseln sowie Zwischenergebnissen der Rekursion. In dem Ver-/Entschlüsselungsmittel 14 sowie dem Rundenschlüsselerzeugungsmittel 18 sind keine Rundenschlüssel speicherbar. Die asynchron zueinander arbeitenden Blöcke Ver-/Entschlüsselungsmittel 14, Steuereinrichtung 12 und Rundenschlüsselerzeugungsmittel 18 kommunizieren über ein Handshake-Protokoll miteinander, wobei keine direkte Datenverbindung zwischen Ver-/Entschlüsselungsmittel 14 und Rundenschlüsselerzeugungsmittel 18 existiert. Zu Beginn einer AES-Berechnung werden alle drei Blöcke parallel gestartet. In das Ver-/Entschlüsselungsmittel 14 werden über einen externen Dateneingang 24 externe Daten eingelesen und der initiale Schlüssel wird über einen externen Schlüsseleingang 22 in die Steuereinrichtung 12 eingelesen. Das Ver-/Entschlüsselungsmittel 14 und das Rundenschlüsselerzeugungsmittel 18 senden beide eine Anforderung an die Steuereinrichtung 12, dass Eingangsdaten benötigt werden und warten, bis diese Anforderung erfüllt ist. Für die erste Ver-/Entschlüsselungsrunde hat das Rundenschlüsselerzeugungsmittel 18 Vorrang, das heißt, es werden die für den rekursiven Algorithmus benötigten Datenworte aus dem Speichermittel 28 gelesen. Für die weiteren Runden kann die Priorität geändert werden. Wenn ein Schlüsselwort berechnet worden ist, wird die Anforderung an die Steuereinrichtung 12 gesendet, dieses Datenwort in das Speichermittel 28 zu schreiben. Das Rundenschlüsselerzeugungsmittel 18 wartet so lange, bis diese Anforderung erfüllt ist. Nun wird der aktuelle Rundenschlüssel an das Ver-/Entschlüsselungsmittel 14 gesendet, die externen Daten werden in dem Ver-/Entschlüsselungsmittel 14 ver- beziehungsweise entschlüsselt und an einen externen Datenausgang 26 bereitgestellt. Um den benötigten Speicherbereich gering zu halten und Siliziumfläche zu sparen, wird mit rotierenden Zeigern gearbeitet, welche bereits gelesene Bereiche wieder zum Schreiben von weiteren Rundenschlüsseln freigeben. Durch die erfindungsgemäßen Mittel wird geringerer Speicherbedarf und eine höhere Sicherheit gegen Attacken auf die Rundenschlüsselerzeugung als bisher bekannt erzielt.

BEZUGSZEICHENLISTE

10	AES-Coprozessor
12	Steuereinrichtung
14	Ver-/Entschlüsselungsmittel
16	Kommunikationsmittel
18	Rundenschlüsselerzeugungsmittel
20	weiteres Kommunikationsmittel
22	externer Schlüsseleingang
24	externer Dateneingang
26	externer Datenausgang
28	Speichermittel

PATENTANSPRÜCHE

1. AES-Coprozessor,
wobei eine Steuereinrichtung (12) mit wenigstens einem Ver-/Entschlüsselungsmittel (14) über wenigstens ein Kommunikationsmittel (16) verbunden ist, die Steuereinrichtung (12) mit wenigstens einem Rundenschlüsselerzeugungsmittel (18) über wenigstens ein weiteres Kommunikationsmittel (20) verbunden ist, die Steuereinrichtung (12) wenigstens einen externen Schlüsseleingang (22) aufweist, das wenigstens eine Ver-/Entschlüsselungsmittel (14) wenigstens einen externen Dateneingang (24) und wenigstens einen externen Datenausgang (26) aufweist und das wenigstens eine Ver-/Entschlüsselungsmittel (14) und das wenigstens eine Rundenschlüsselerzeugungsmittel (18) voneinander entkoppelt sind.

2. AES-Coprozessor nach Anspruch 1,
dadurch gekennzeichnet,
dass das wenigstens eine Kommunikationsmittel (16) wenigstens eine Anforderungsleitung, wenigstens eine Freigabeleitung und wenigstens eine Datenleitung und/oder das wenigstens eine weitere Kommunikationsmittel (20) wenigstens eine weitere Anforderungsleitung, wenigstens eine weitere Freigabeleitung und wenigstens eine weitere Datenleitung umfasst.

3. AES-Coprozessor nach einem der vorhergehenden Ansprüche,
dadurch gekennzeichnet,
dass die wenigstens eine Anforderungsleitung, die wenigstens eine Freigabeleitung und die wenigstens eine Datenleitung und/oder die wenigstens eine weitere Anforderungsleitung, die wenigstens eine weitere Freigabeleitung und die wenigstens eine weitere Datenleitung zumindest teilweise dieselbe Leitungsphysik belegen.

4. AES-Coprozessor nach einem der vorhergehenden Ansprüche,
dadurch gekennzeichnet,
dass die Steuereinrichtung (12) wenigstens ein Speichermittel (28) umfasst, in welchem wenigstens ein mittels des wenigstens einen Rundenschlüsselerzeugungsmittels (18) erzeugter Rundenschlüssel temporär speicherbar ist.

5. AES-Coprozessor nach Anspruch 4,
dadurch gekennzeichnet,
dass für den Zugriff auf das wenigstens eine Speichermittel (28) wenigstens ein rotierender Zeiger vorgesehen ist.

6. AES-Coprozessor nach einem der vorhergehenden Ansprüche,
dadurch gekennzeichnet,
dass zur Kommunikation der Steuereinrichtung (12) mit dem wenigstens einen Ver-/Entschlüsselungsmittel (14) und/oder mit dem wenigstens einen Rundenschlüsselerzeugungsmittel (18) wenigstens ein Handshake-Protokoll vorgesehen ist.

7. AES-Coprozessor nach einem der vorhergehenden Ansprüche,
dadurch gekennzeichnet,
dass die Arbeitsweise der Steuereinrichtung (12), des wenigstens eine Ver-/Entschlüsselungsmittels (14) und des wenigstens einen Rundenschlüsselerzeugungsmittels (18) asynchron zueinander ist.

8. AES-Coprozessor nach einem der vorhergehenden Ansprüche,
dadurch gekennzeichnet,
dass mittels des wenigstens einen Rundenschlüsselerzeugungsmittels (18) während wenigstens einer inaktiven Phase wenigstens eine Dummy-Berechnung und/oder wenigstens ein Teil wenigstens einer früheren Rundenschlüsselberechnung durchführbar ist.

9. AES-Coprozessor nach einem der vorhergehenden Ansprüche,
dadurch gekennzeichnet,
dass die Zeitspanne zwischen Berechnung und Verwendung des wenigstens einen Rundenschlüssels variabel ist.

10. Verfahren zur AES-Berechnung unter Verwendung eines AES-Coprozessors nach wenigstens einem der Ansprüche 1 bis 9,
wobei

a) wenigstens ein initialer Schlüssel in eine Steuereinrichtung eingelesen wird,
b) externe Daten in wenigstens ein Ver-/Entschlüsselungsmittel eingelesen werden,
c) wenigstens ein zur Berechnung wenigstens eines Rundenschlüssels benötigtes Datenwort aus wenigstens einem Speichermittel der Steuereinrichtung ausgelesen und zu wenigstens einem Rundenschlüsselerzeugungsmittel transferiert wird,
d) wenigstens ein Rundenschlüssel auf Basis des wenigstens einen Datenwortes mittels des wenigstens einen Rundenschlüsselerzeugungsmittels rekursiv berechnet, zur Steuereinrichtung transferiert und in dem wenigstens einen Speichermittel gespeichert wird,
e) der wenigstens eine Rundenschlüssel zu dem wenigstens einen Ver-/Entschlüsselungsmittel transferiert wird,
f) die externen Daten mittels des wenigstens einen Ver-/Entschlüsselungsmittels unter Verwendung des wenigstens einen Rundenschlüssels verschlüsselt oder entschlüsselt und die ver- beziehungsweise entschlüsselten Daten an wenigstens einem externen Datenausgang bereitgestellt werden und
g) die Schritte b) bis f) so oft wie zur Ver- beziehungsweise Entschlüsselung eines Satzes externer Daten erforderlich wiederholt werden.

11. Verfahren nach Anspruch 10,
dadurch gekennzeichnet,
dass die Kommunikation der Steuereinrichtung mit dem wenigstens einen Ver-/Entschlüsselungsmittel und/oder dem wenigstens einen Rundenschlüsselerzeugungsmittel mittels wenigstens eines Handshake-Protokolls erfolgt.

12. Verfahren nach einem der Ansprüche 10 bis 11,
dadurch gekennzeichnet,
dass die Kommunikation der Steuereinrichtung mit dem wenigstens einen Ver-/Entschlüsselungsmittel und dem wenigstens einen Rundenschlüsselerzeugungsmittel asynchron erfolgt.

13. Verfahren nach einem der Ansprüche 10 bis 12,
dadurch gekennzeichnet,
dass der Zugriff auf das wenigstens eine Speichermittel mittels wenigstens eines rotierenden Zeigers erfolgt.

14. Verfahren nach einem der Ansprüche 10 bis 13,
dadurch gekennzeichnet,
dass mittels des wenigstens einen Rundenschlüsselerzeugungsmittels während wenigstens einer inaktiven Phase wenigstens eine Dummy-Berechnung und/oder wenigstens ein Teil wenigstens einer früheren Rundenschlüsselberechnung durchgeführt wird.

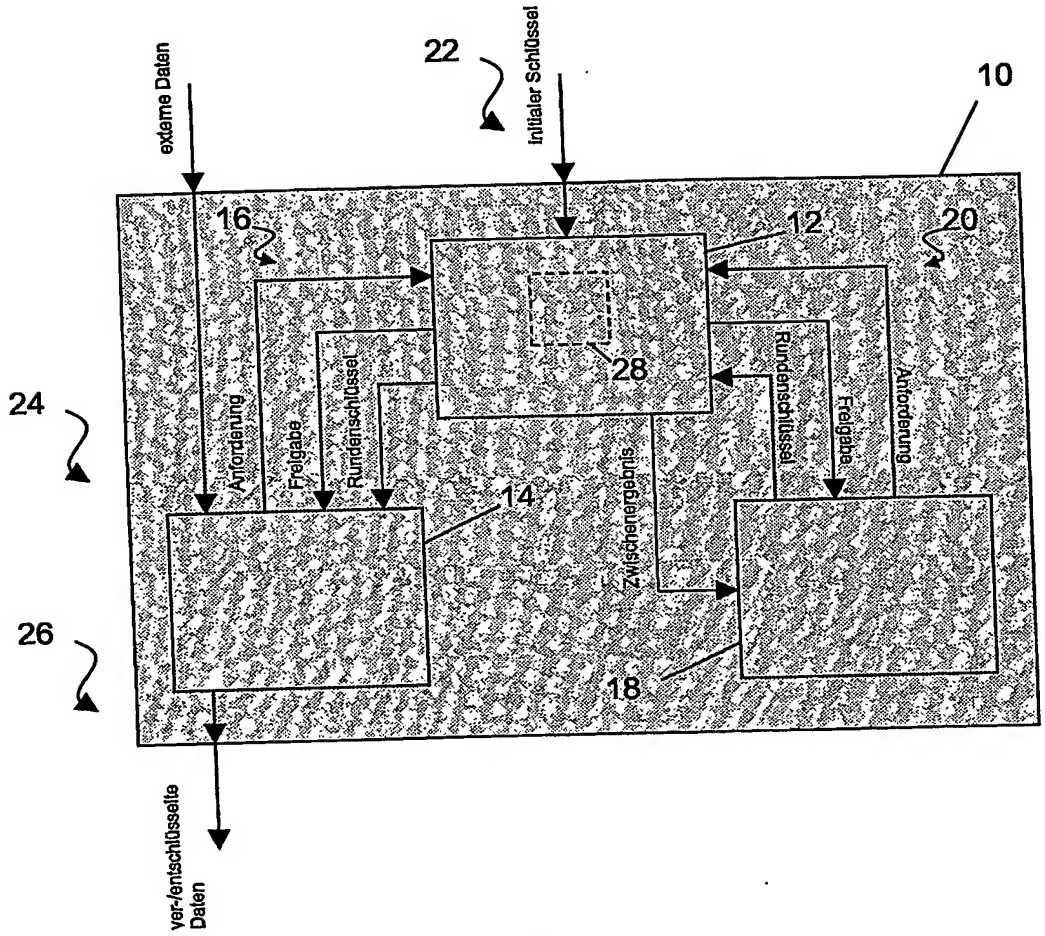
15. Verfahren nach einem der Ansprüche 10 bis 14,
dadurch gekennzeichnet,
dass die Zeitspanne zwischen Berechnung und Verwendung des wenigstens einen Rundenschlüssels variabel ist.

ZUSAMMENFASSUNG

AES-Coprozessor und Verfahren zur AES-Berechnung

Um einen AES-Coprozessor und ein Verfahren zur AES-Berechnung zu schaffen, welche sich durch einen geringeren Speicherbedarf und eine höhere Sicherheit gegen Attacken auf die Rundenschlüsselerzeugung als bisher bekannt auszeichnen, ist vorgesehen, dass eine Steuereinrichtung (12) mit wenigstens einem Ver-/Entschlüsselungsmittel (14) über wenigstens ein Kommunikationsmittel (16) verbunden ist, die Steuereinrichtung (12) mit wenigstens einem Rundenschlüsselerzeugungsmittel (18) über wenigstens ein weiteres Kommunikationsmittel (20) verbunden ist, die Steuereinrichtung (12) wenigstens einen externen Schlüsseleingang (22) aufweist, das wenigstens eine Ver-/Entschlüsselungsmittel (14) wenigstens einen externen Dateneingang (24) und wenigstens einen externen Datenausgang (26) aufweist und das wenigstens eine Ver-/Entschlüsselungsmittel (14) und das wenigstens eine Rundenschlüsselerzeugungsmittel (18) voneinander entkoppelt sind. Das erfindungsgemäße Verfahren sieht vor, dass wenigstens ein initialer Schlüssel in eine Steuereinrichtung eingelesen wird, externe Daten in wenigstens ein Ver-/Entschlüsselungsmittel eingelesen werden, wenigstens ein zur Berechnung wenigstens eines Rundenschlüssels benötigtes Datenwort aus wenigstens einem Speichermittel der Steuereinrichtung ausgelesen und zu wenigstens einem Rundenschlüsselerzeugungsmittel transferiert wird, wenigstens ein Rundenschlüssel auf Basis des wenigstens einen Datenwortes mittels des wenigstens einen Rundenschlüsselerzeugungsmittels rekursiv berechnet, zur Steuereinrichtung transferiert und in dem wenigstens einen Speichermittel gespeichert wird, der wenigstens eine Rundenschlüssel zu dem wenigstens einen Ver-/Entschlüsselungsmittel transferiert wird, die externen Daten mittels des wenigstens einen Ver-/Entschlüsselungsmittels unter Verwendung des wenigstens einen Rundenschlüssels verschlüsselt oder entschlüsselt und die ver- beziehungsweise entschlüsselten Daten an wenigstens einem externen Datenausgang bereitgestellt werden und diese Schritte so oft wie zur Ver- beziehungsweise Entschlüsselung eines Satzes externer Daten erforderlich wiederholt werden.

Fig.


externe Daten
22
Initialer Schlüssel
10
16
12
20
28
24
Anforderung
Freigabe
Rundenschlüssel
14
Zwischenergebnis
Rundenschlüssel
Freigabe
Anforderung
26
18
ver-/entschlüsselte Daten

Figur